U.S. Department of State, Information Resource Management,

Office of Information Assurance, November16, 2010

John Streufert (DOSCISO@state.gov)

Deputy Chief Information Officer for Information Security

FISMA 2.0: Toward lower risk, faster patching & higher ROI

Nature of Attacks

80% of attacks leverage known vulnerabilities and configuration management setting weaknesses

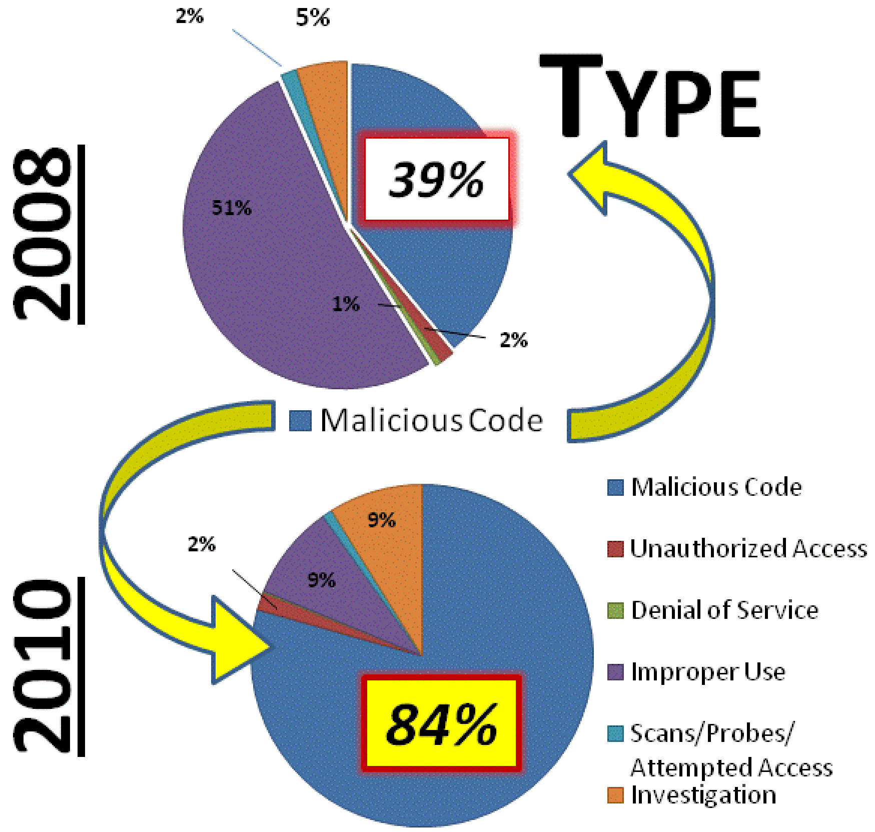
Tickets

Threats Increasing

TICKETS

Year	Tickets
2008	*2104*
2009	*3085*
2010	*+6000 ** *projected*

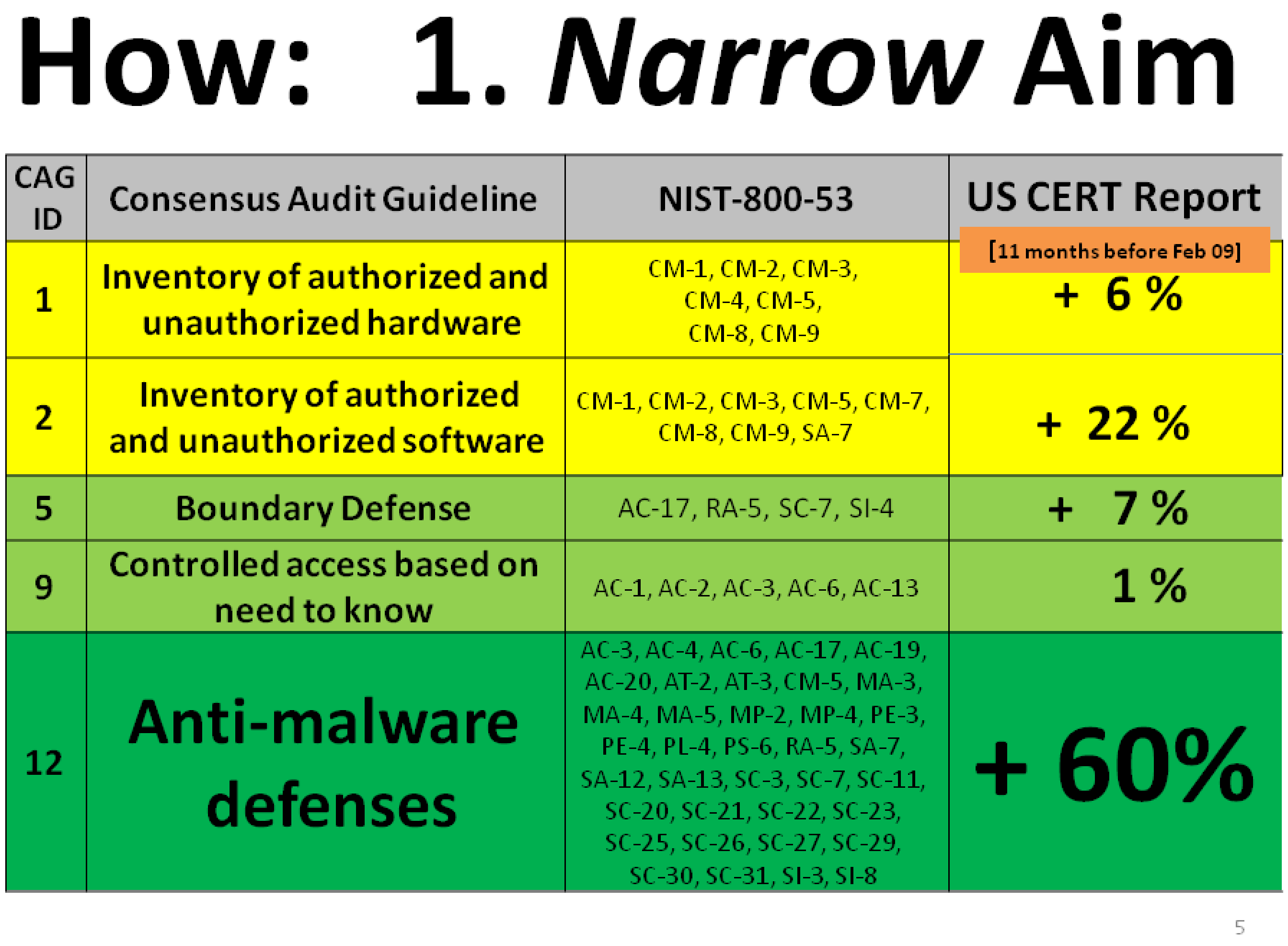
* 3000 by June 2010



Case Study:

- Scan every 2 – 7* days
- Find & Fix Top Issues Daily
- Personal results graded
- Hold managers responsible

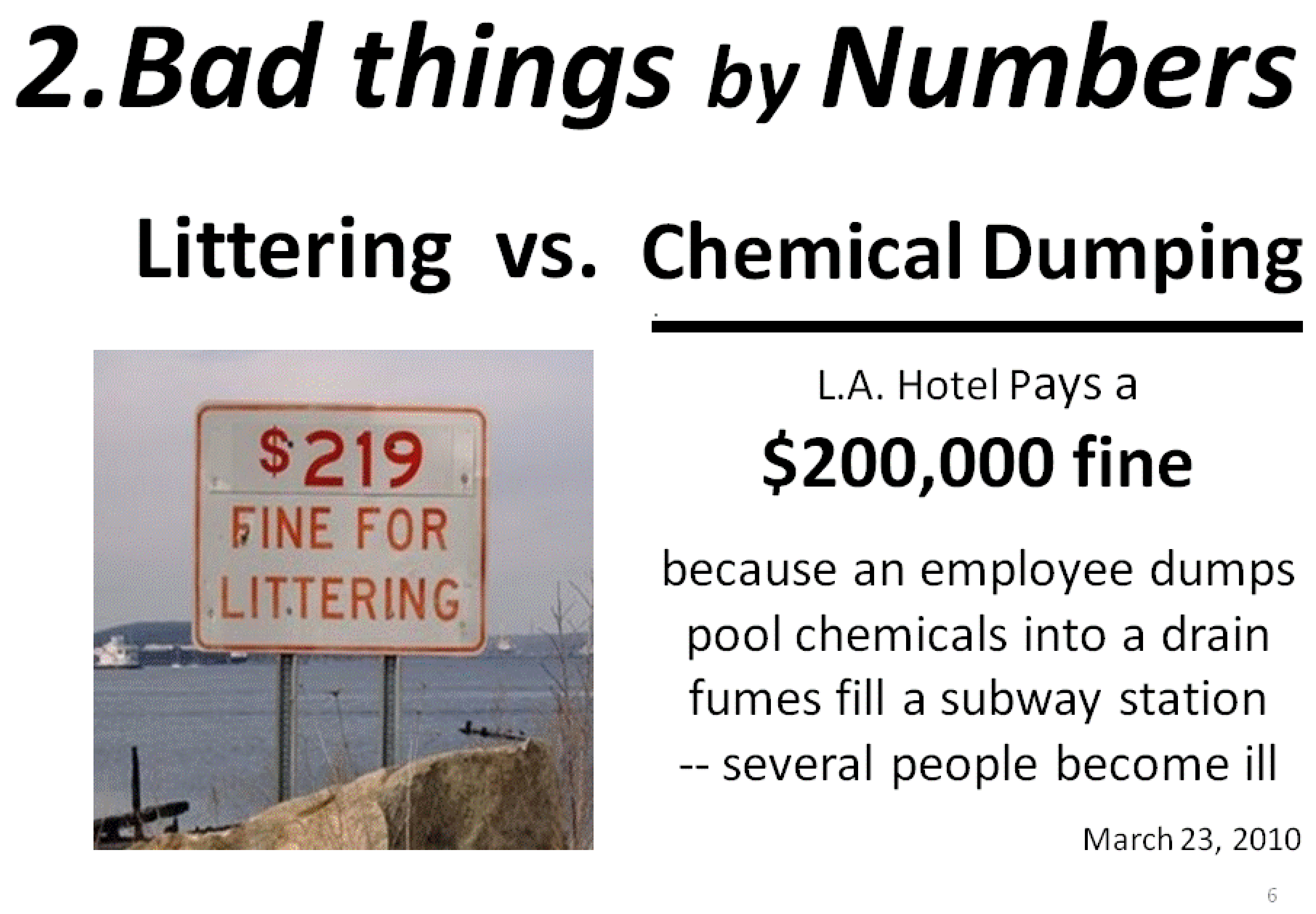
How: 1. *Narrow* Aim



How: 1. *Narrow* Aim

CAG ID	Consensus Audit Guideline	NIST-800-53	US CERT Report [11 months before Feb 09]
1	Inventory of authorized and unauthorized hardware	CM-1, CM-2, CM-3, CM-4, CM-5, CM-8, CM-9	+ 6 %
2	Inventory of authorized and unauthorized software	CM-1, CM-2, CM-3, CM-5, CM-7, CM-8, CM-9, SA-7	+ 22 %
5	Boundary Defense	AC-17, RA-5, SC-7, SI-4	+ 7 %
9	Controlled access based on need to know	AC-1, AC-2, AC-3, AC-6, AC-13	1 %
12	Anti-malware defenses	AC-3, AC-4, AC-6, AC-17, AC-19, AC-20, AT-2, AT-3, CM-5, MA-3, MA-4, MA-5, MP-2, MP-4, PE-3, PE-4, PL-4, PS-6, RA-5, SA-7, SA-12, SA-13, SC-3, SC-7, SC-11, SC-20, SC-21, SC-22, SC-23, SC-25, SC-26, SC-27, SC-29, SC-30, SC-31, SI-3, SI-8	+ 60%

2. Bad things by Numbers



$219
FINE FOR
LITTERING

2. *Bad things* by *Numbers*

Littering vs. Chemical Dumping

L.A. Hotel Pays a

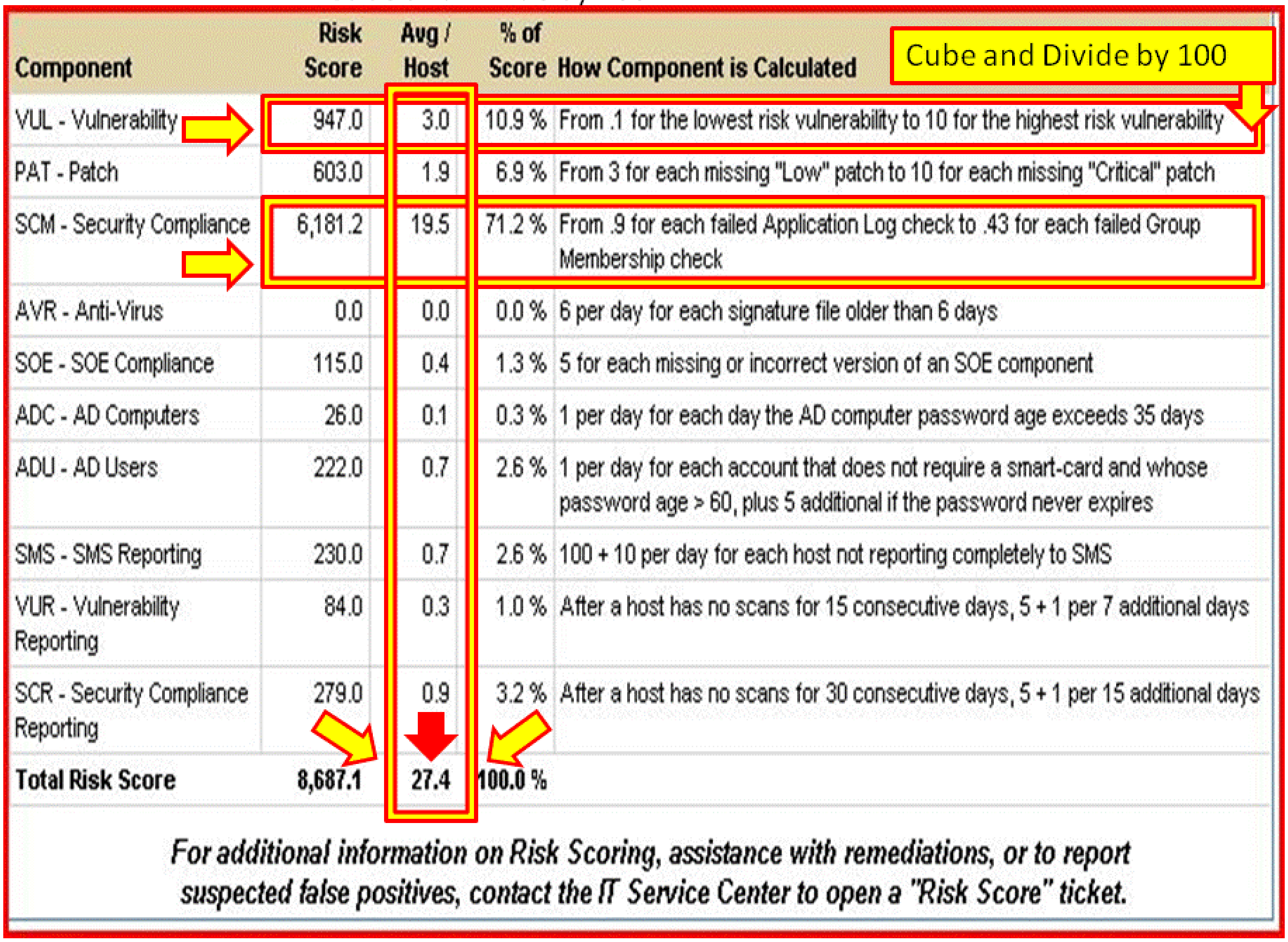
$200,000 fine

because an employee dumps pool chemicals into a drain fumes fill a subway station -- several people become ill

March 23, 2010

Cube and Divide by 100

Cube and Divide by 100



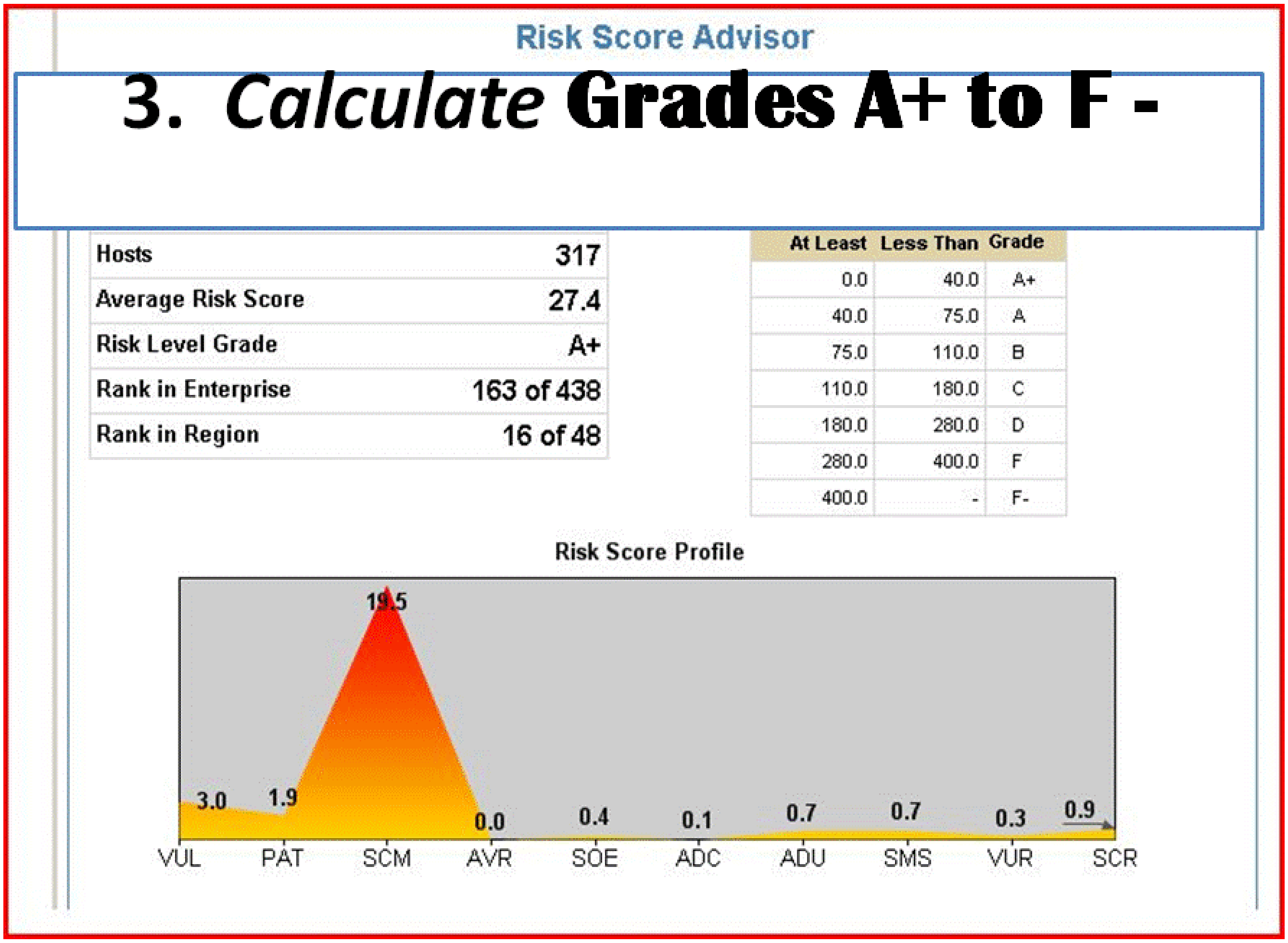
Cube and Divide by 100

Component	Risk Score	Avg / Host	% of Score	How Component is Calculated
VUL - Vulnerability	947.0	3.0	10.9 %	From .1 for the lowest risk vulnerability to 10 for the highest risk vulnerability
PAT - Patch	603.0	1.9	6.9 %	From 3 for each missing "Low" patch to 10 for each missing "Critical" patch
SCM - Security Compliance	6,181.2	19.5	71.2 %	From .9 for each failed Application Log check to .43 for each failed Group Membership check
AVR - Anti-Virus	0.0	0.0	0.0 %	6 per day for each signature file older than 6 days
SOE - SOE Compliance	115.0	0.4	1.3 %	5 for each missing or incorrect version of an SOE component
ADC - AD Computers	26.0	0.1	0.3 %	1 per day for each day the AD computer password age exceeds 35 days
ADU - AD Users	222.0	0.7	2.6 %	1 per day for each account that does not require a smart-card and whose password age > 60, plus 5 additional if the password never expires
SMS - SMS Reporting	230.0	0.7	2.6 %	100 + 10 per day for each host not reporting completely to SMS
VUR - Vulnerability Reporting	84.0	0.3	1.0 %	After a host has no scans for 15 consecutive days, 5 + 1 per 7 additional days
SCR - Security Compliance Reporting	279.0	0.9	3.2 %	After a host has no scans for 30 consecutive days, 5 + 1 per 15 additional days
Total Risk Score	**8,687.1**	**27.4**	**100.0 %**	

For additional information on Risk Scoring, assistance with remediations, or to report suspected false positives, contact the IT Service Center to open a "Risk Score" ticket.

3. Calculate Grades A+ to F –

3. *Calculate* Grades A+ to F -



Risk Score Advisor

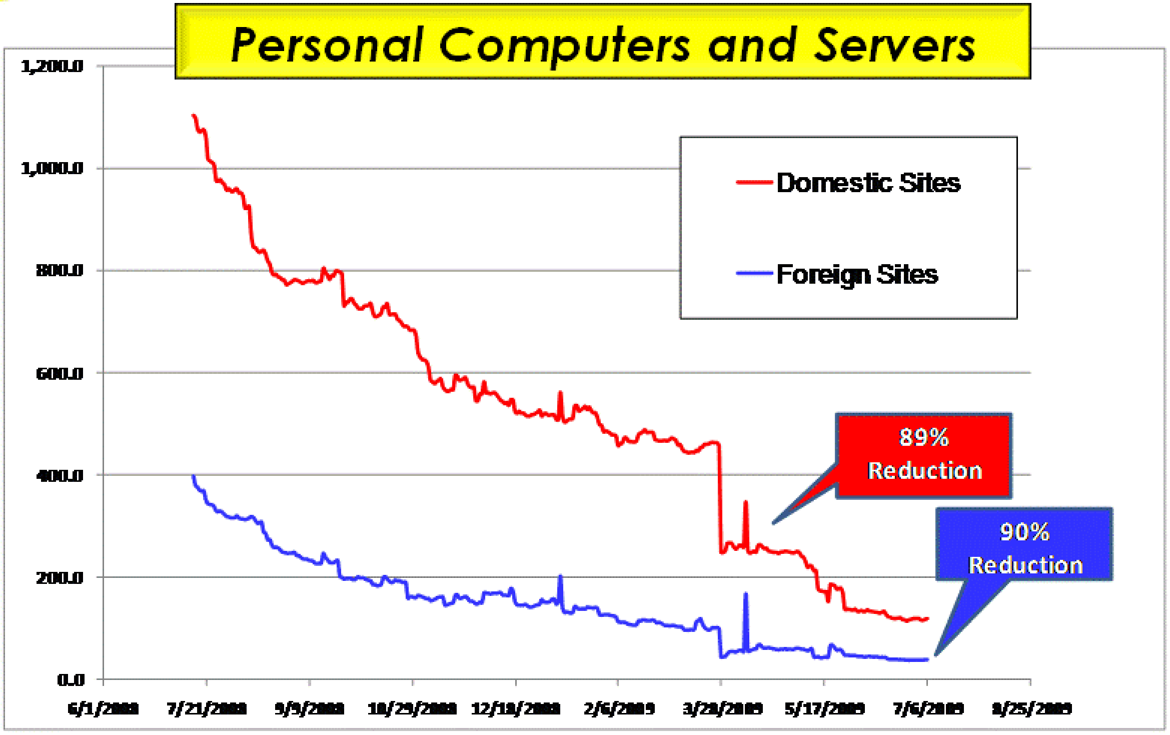
Hosts	317
Average Risk Score	27.4
Risk Level Grade	A+
Rank in Enterprise	163 of 438
Rank in Region	16 of 48

At Least	Less Than	Grade
0.0	40.0	A+
40.0	75.0	A
75.0	110.0	B
110.0	180.0	C
180.0	280.0	D
280.0	400.0	F
400.0	-	F-

Risk Score Profile

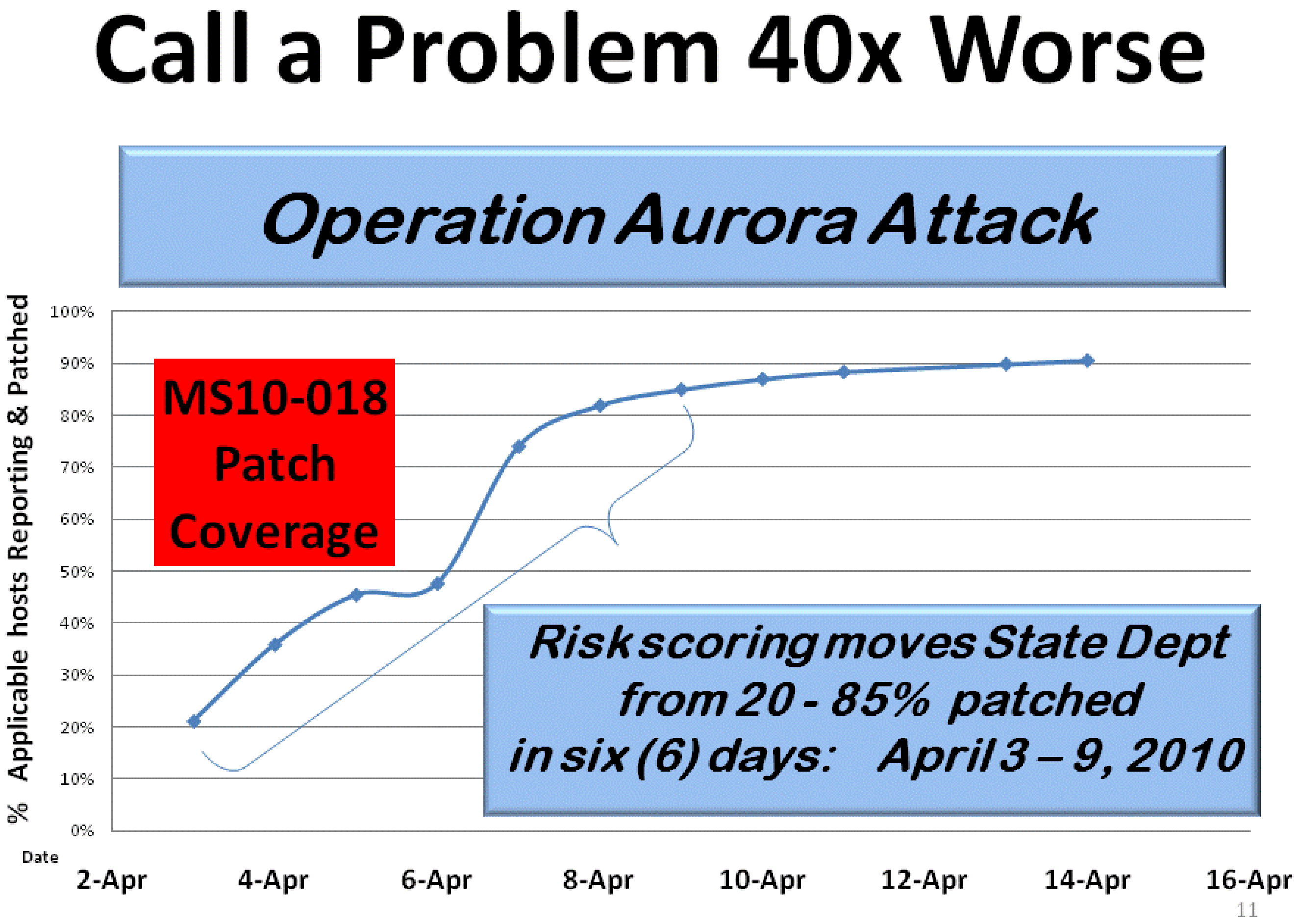
Results First 12 Months

Results First 12 Months



Risk Scoring in 2nd Year

Operation Aurora Attack



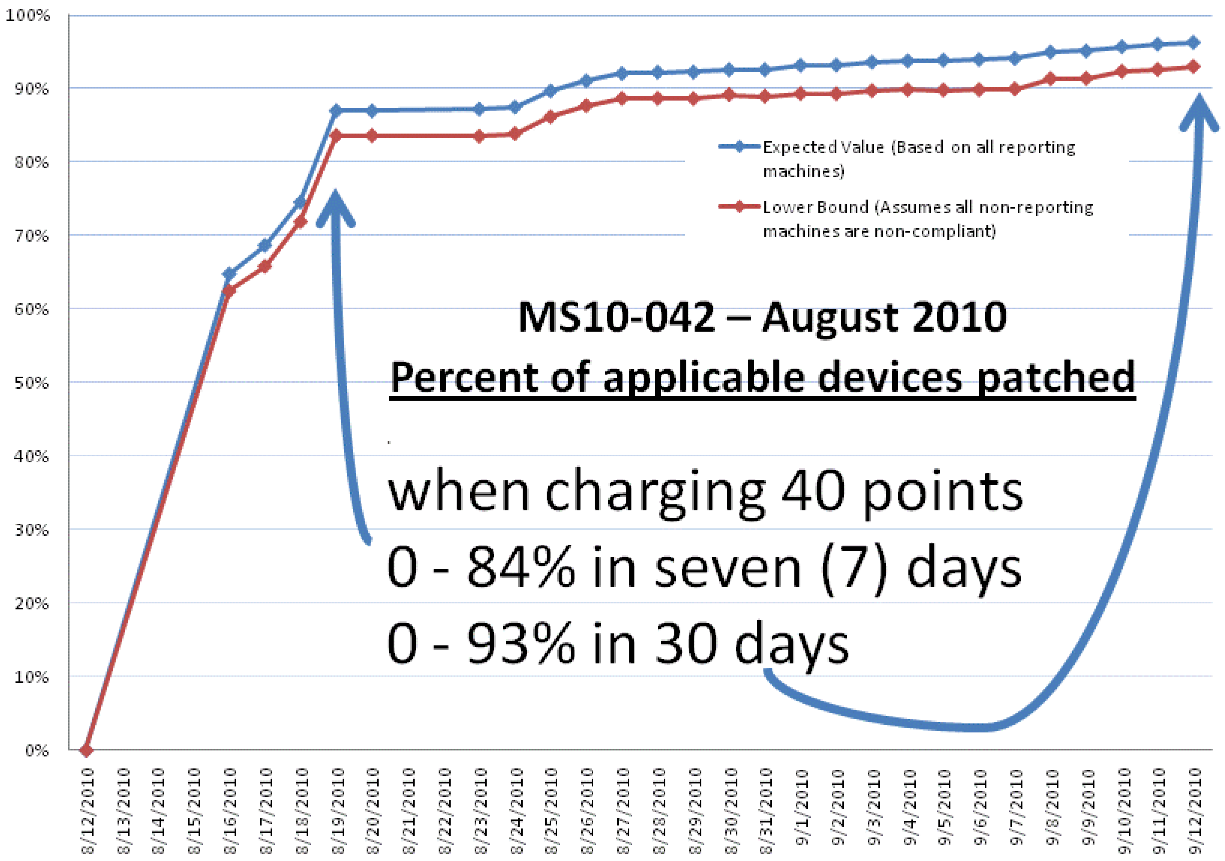
Call a Problem 40x Worse

Operation Aurora Attack

Risk scoring moves State Dept from 20 - 85% patched in six (6) days: April 3 – 9, 2010

Efficiency is Repeatable & Sustained

Efficiency is Repeatable & Sustained



MS10-042 – August 2010

Percent of applicable devices patched

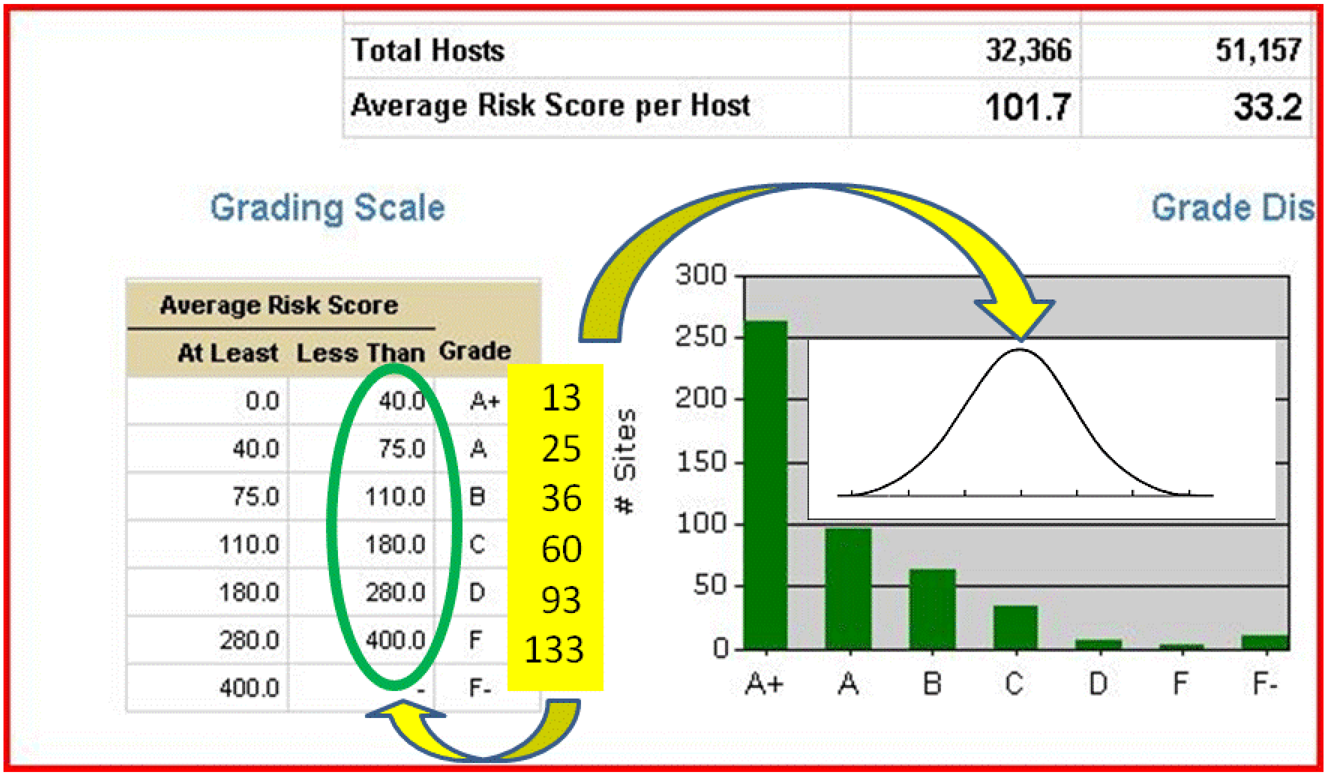
when charging 40 points

0 - 84% in seven (7) days

0 - 93% in 30 days

Risk Score Monitor Enterprise

Risk Score Monitor Enterprise



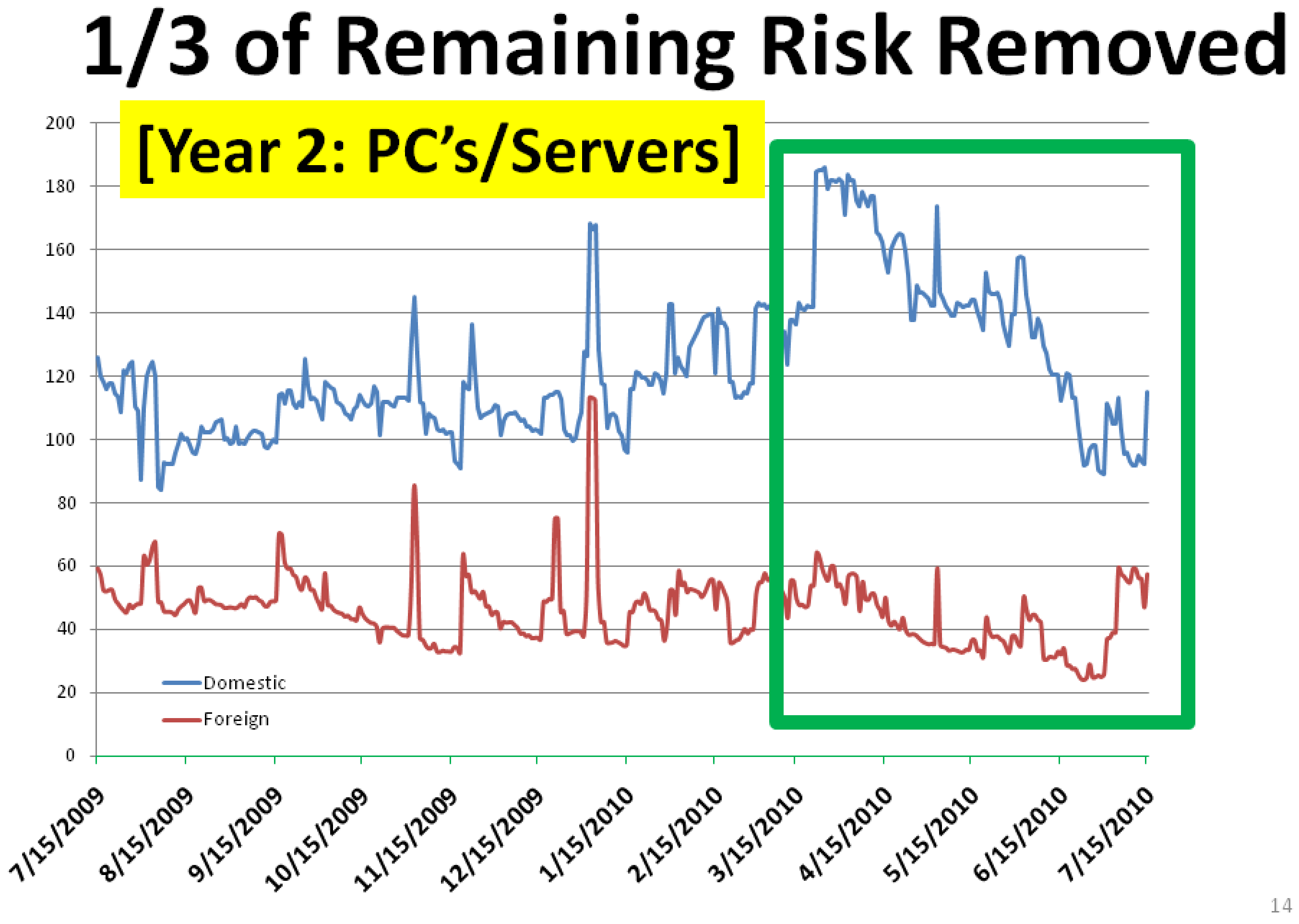
Total Hosts	32,366	51,157
Average Risk Score per Host	101.7	33.2

Grading Scale

Average Risk Score			
At Least	Less Than	Grade	
0.0	40.0	A+	13
40.0	75.0	A	25
75.0	110.0	B	36
110.0	180.0	C	60
180.0	280.0	D	93
280.0	400.0	F	133
400.0	-	F-	

Grade Dis

1/3 of Remaining Risk Removed

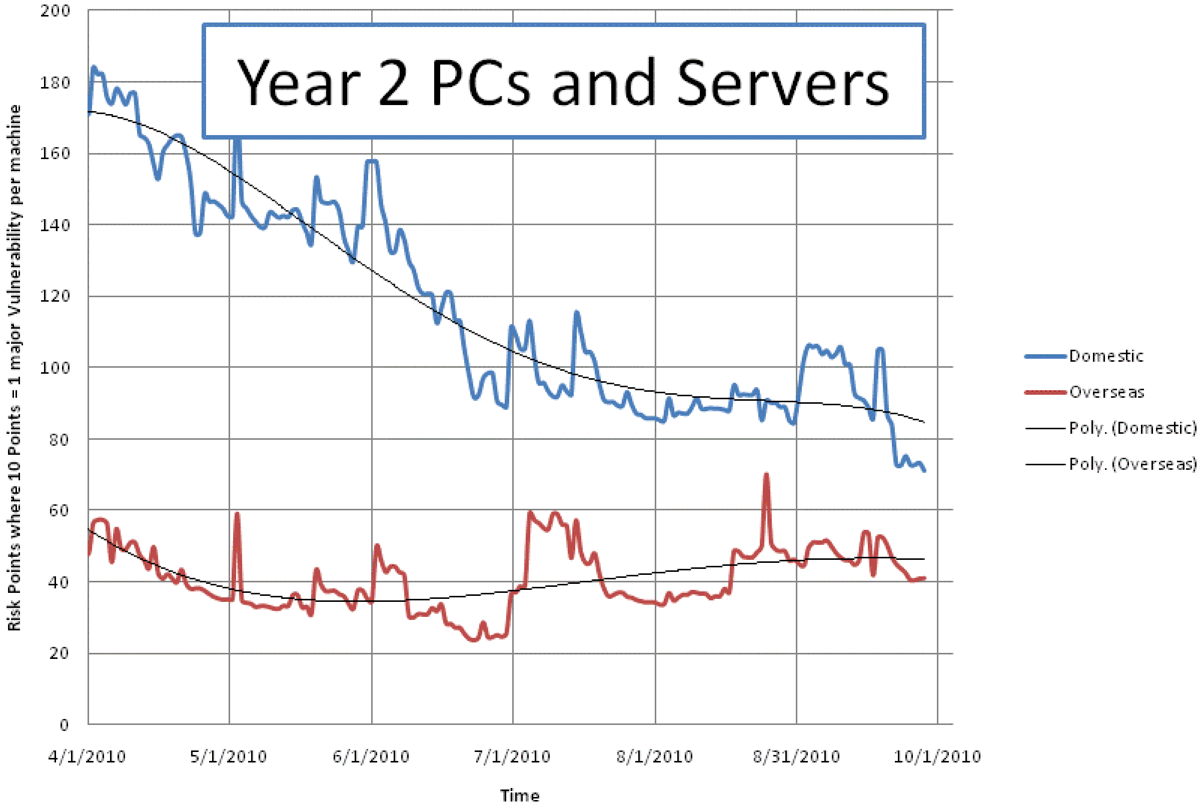


1/3 of Remaining Risk Removed

[Year 2: PC’s/Servers]

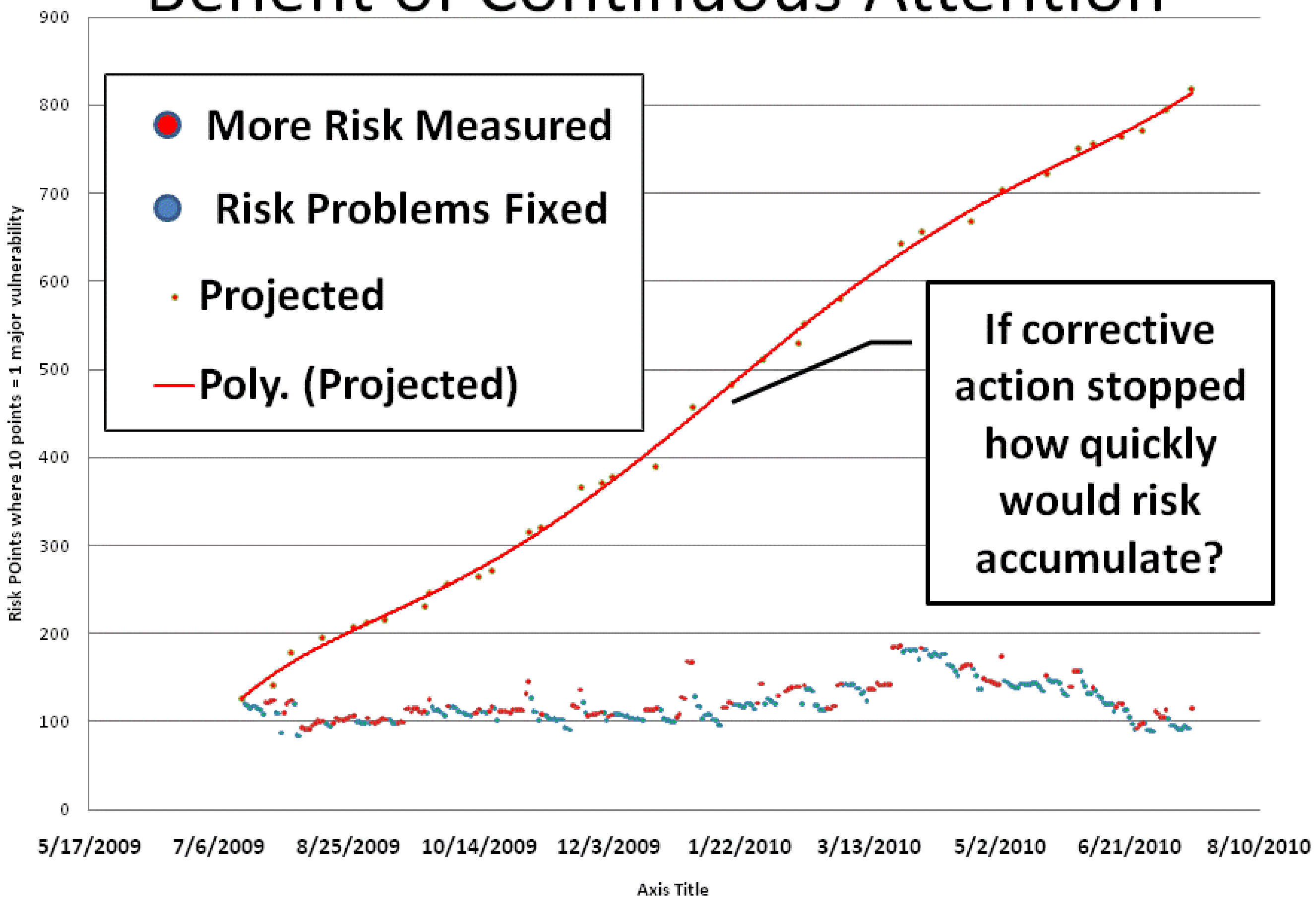
Year 2 PCs and Servers

Grade	Now	April	May	June	July	Aug	Sep
A+	40	36	31	27	22	18	13


Year 2 PCs and Servers

Benefit of Continuous Attention

Benefit of Continuous Attention



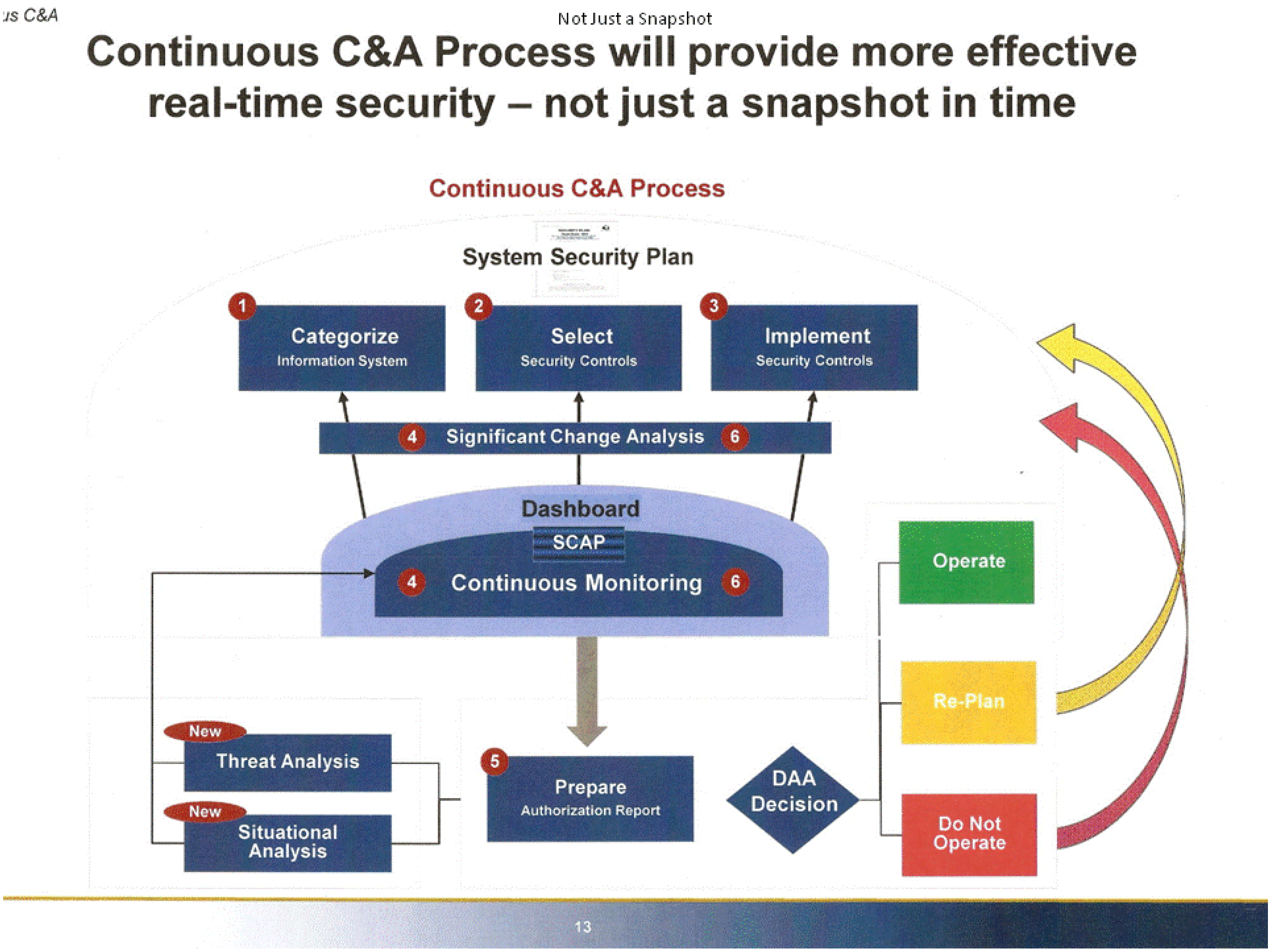
If corrective action stopped how quickly would risk accumulate?

Lessons Learned

- When **continuous monitoring** augments snapshots required by FISMA:
  - Mobilizing to lower risk is feasible & fast (11 mo)
  - Changes in 24 time zones with no direct contact
  - Cost: 15 FTE above technical management base
- This approach leverages the wider workforce
- Security culture gains are grounded in fairness, commitment and personal accountability for improvement

Next Steps

Not Just a Snapshot



Not Just a Snapshot

Continuous C&A Process will provide more effective real-time security – not just a snapshot in time

Continuous C&A Pilots

a. Inventory of Authorized Assets (CAG 1/2)

b. Configuration and Vulnerability Monitoring

(CAG 3/4/10/12/13)

a. SCAP Content (automated & non-automated testing)

b. Boundary Defense (CAG 5/14)

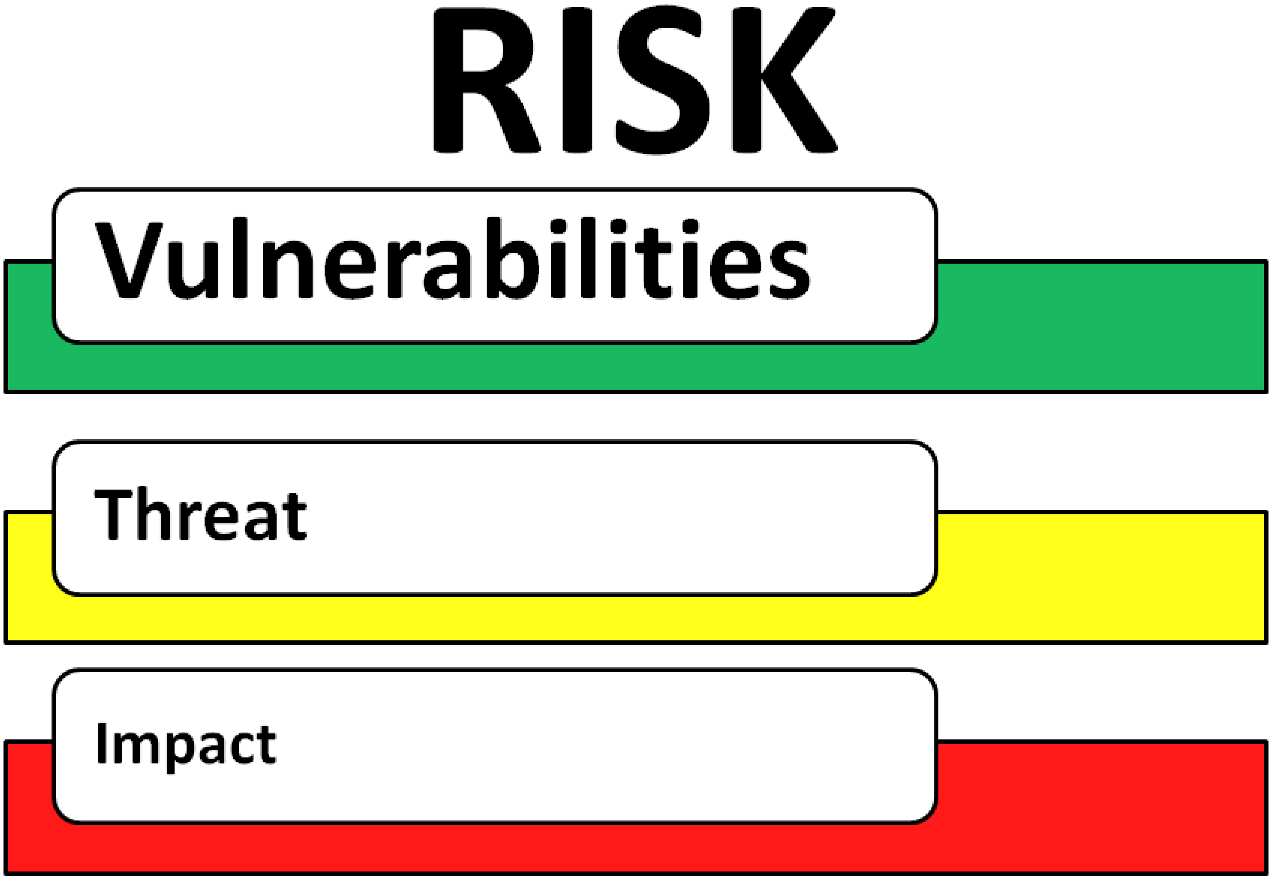
c. Situational Awareness and Threat Analysis

d. Applications (CAG 7)

e. Access Controls (CAG 6/8/9/11)

f. Data Loss Protection (CAG 15)

Risk



RISK

Vulnerabilities

Threat

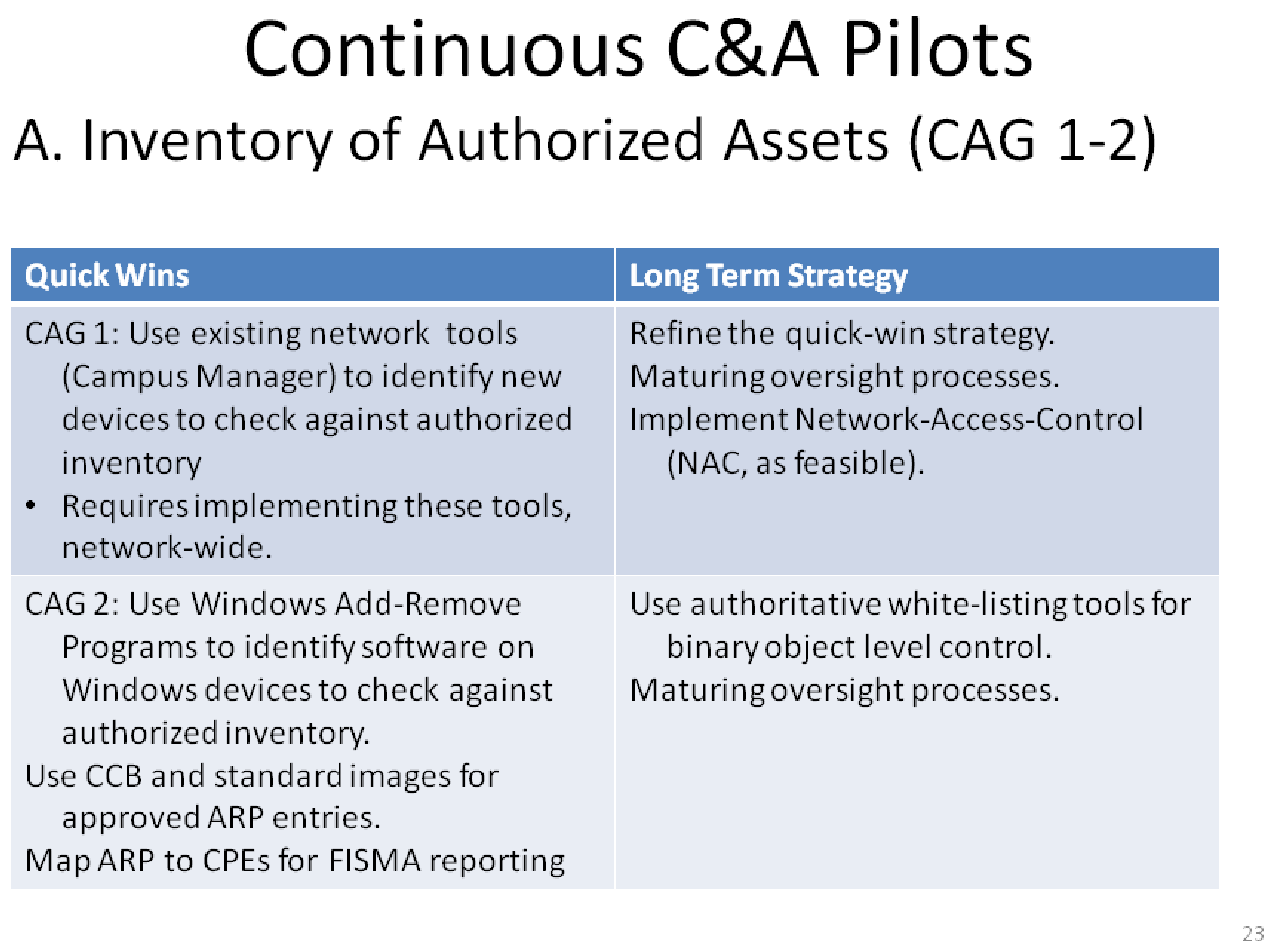
Impact

Conclusions

- **Scalable to large complex public and private sector organizations**
- **Higher ROI for continuous monitoring of technical controls as a substitute for paper reports**
- Summarized risk estimates could be fed to enterprise level reporting

Continuous C&A Pilots

A. Inventory of Authorized Assets (CAG 1-2)

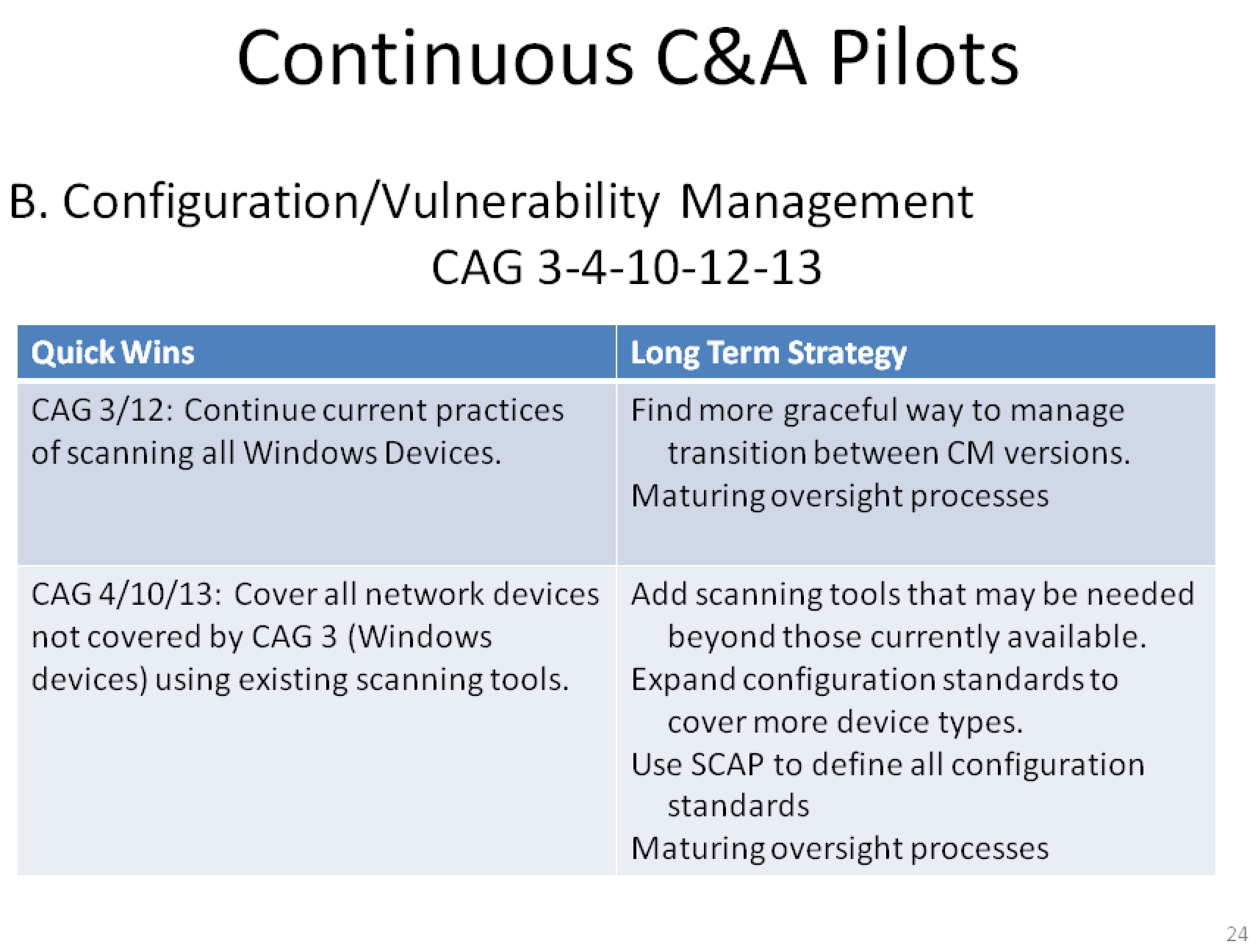


Continuous C&A Pilots

A. Inventory of Authorized Assets (CAG 1-2)

Quick Wins	Long Term Strategy
CAG 1: Use existing network tools (Campus Manager) to identify new devices to check against authorized inventory • Requires implementing these tools, network-wide.	Refine the quick-win strategy. Maturing oversight processes. Implement Network-Access-Control (NAC, as feasible).
CAG 2: Use Windows Add-Remove Programs to identify software on Windows devices to check against authorized inventory. Use CCB and standard images for approved ARP entries. Map ARP to CPEs for FISMA reporting	Use authoritative white-listing tools for binary object level control. Maturing oversight processes.

B. Configuration/Vulnerability Management (CAG 3-4-10-12-13)

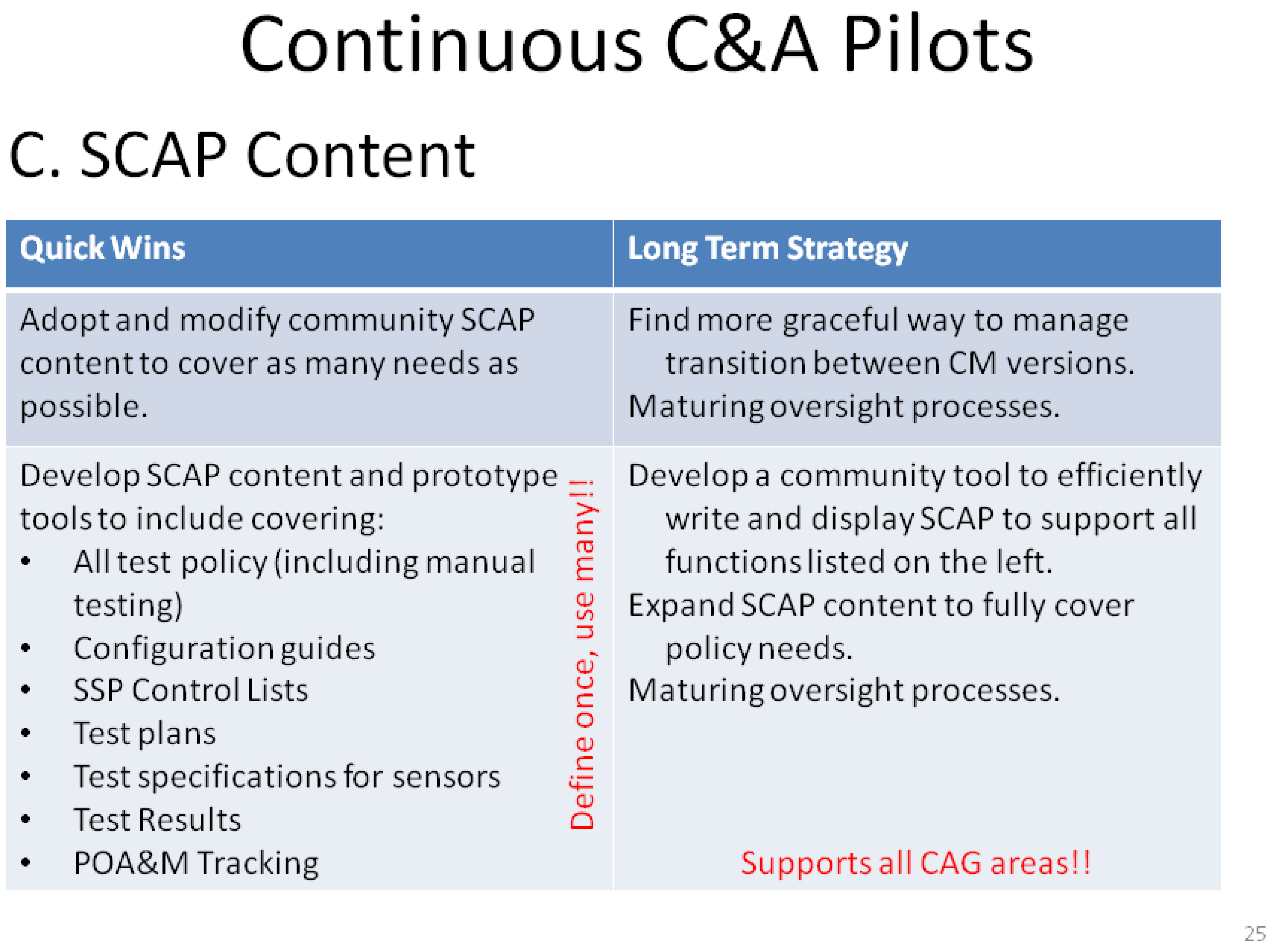


Continuous C&A Pilots

B. Configuration/Vulnerability Management CAG 3-4-10-12-13

Quick Wins	Long Term Strategy
CAG 3/12: Continue current practices of scanning all Windows Devices.	Find more graceful way to manage transition between CM versions. Maturing oversight processes
CAG 4/10/13: Cover all network devices not covered by CAG 3 (Windows devices) using existing scanning tools.	Add scanning tools that may be needed beyond those currently available. Expand configuration standards to cover more device types. Use SCAP to define all configuration standards Maturing oversight processes

C. SCAP Content



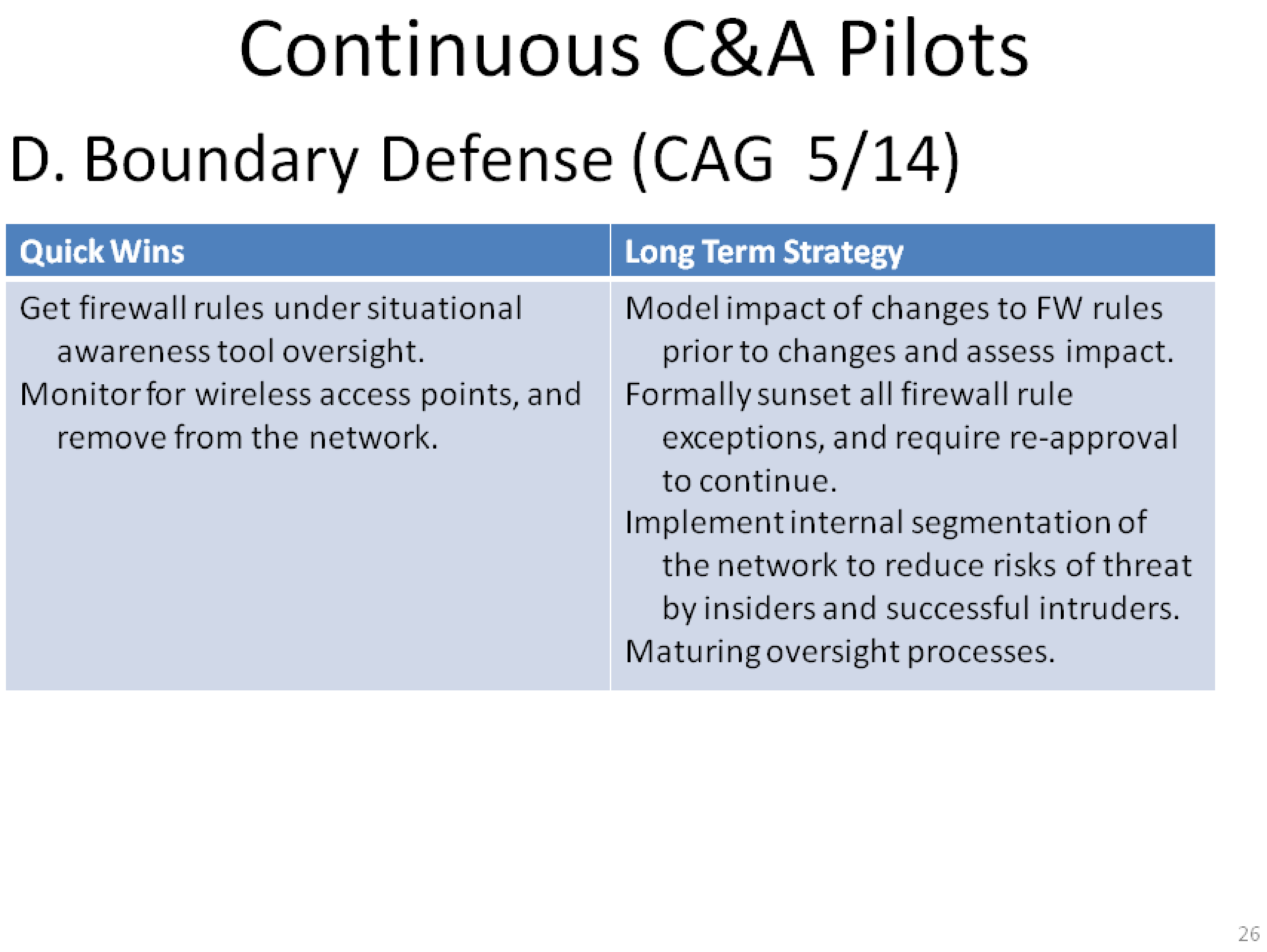
Continuous C&A Pilots

C. SCAP Content

Quick Wins	Long Term Strategy
Adopt and modify community SCAP content to cover as many needs as possible.	Find more graceful way to manage transition between CM versions. Maturing oversight processes.
Develop SCAP content and prototype tools to include covering: • All test policy (including manual testing) • Configuration guides • SSP Control Lists • Test plans • Test specifications for sensors • Test Results • POA&M Tracking Define once, use many!!	Develop a community tool to efficiently write and display SCAP to support all functions listed on the left. Expand SCAP content to fully cover policy needs. Maturing oversight processes. Supports all CAG areas!!

25

D. Boundary Defense (CAG 5/14)

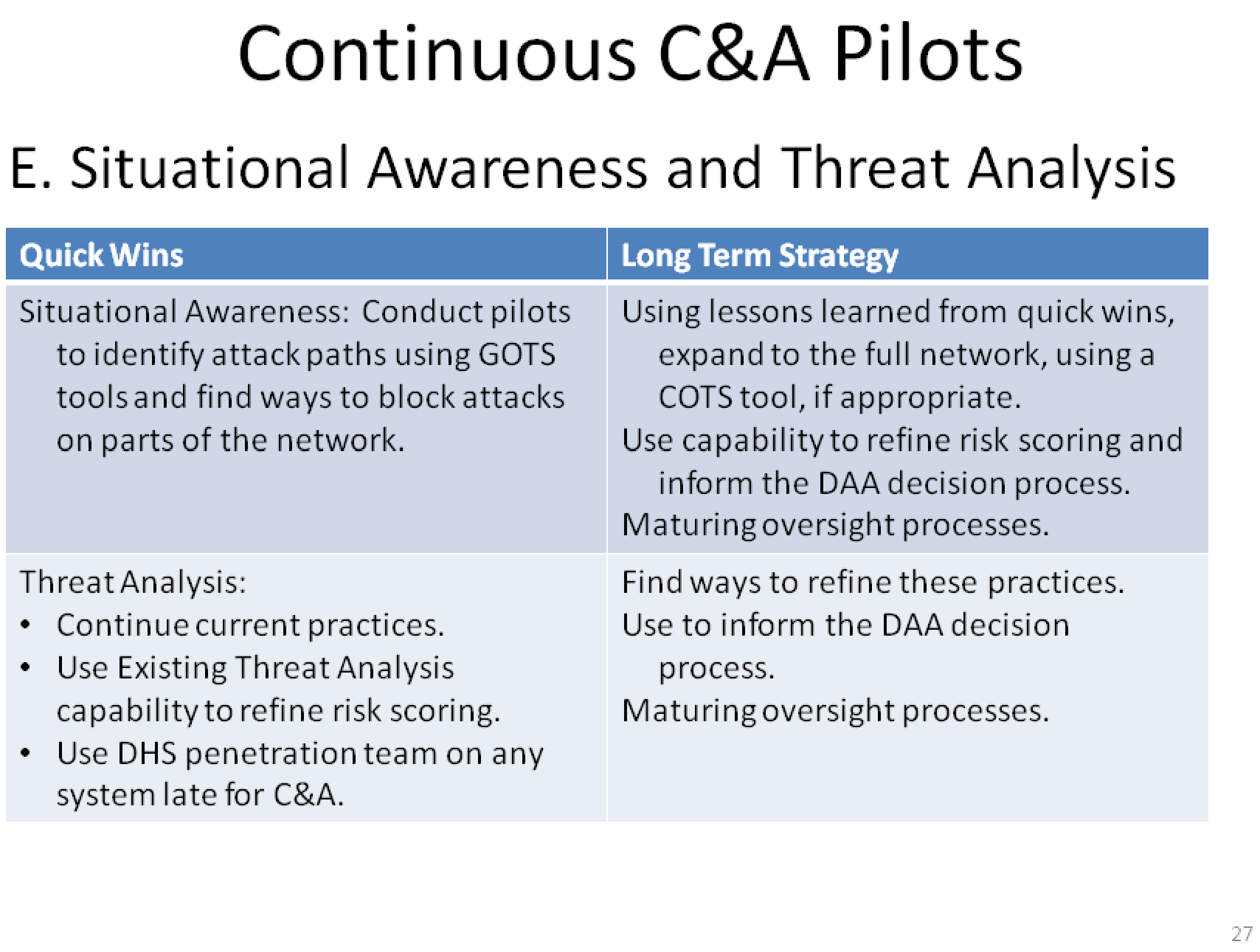


Continuous C&A Pilots

D. Boundary Defense (CAG 5/14)

Quick Wins	Long Term Strategy
Get firewall rules under situational awareness tool oversight. Monitor for wireless access points, and remove from the network.	Model impact of changes to FW rules prior to changes and assess impact. Formally sunset all firewall rule exceptions, and require re-approval to continue. Implement internal segmentation of the network to reduce risks of threat by insiders and successful intruders. Maturing oversight processes.

E. Situational Awareness and Threat Analysis

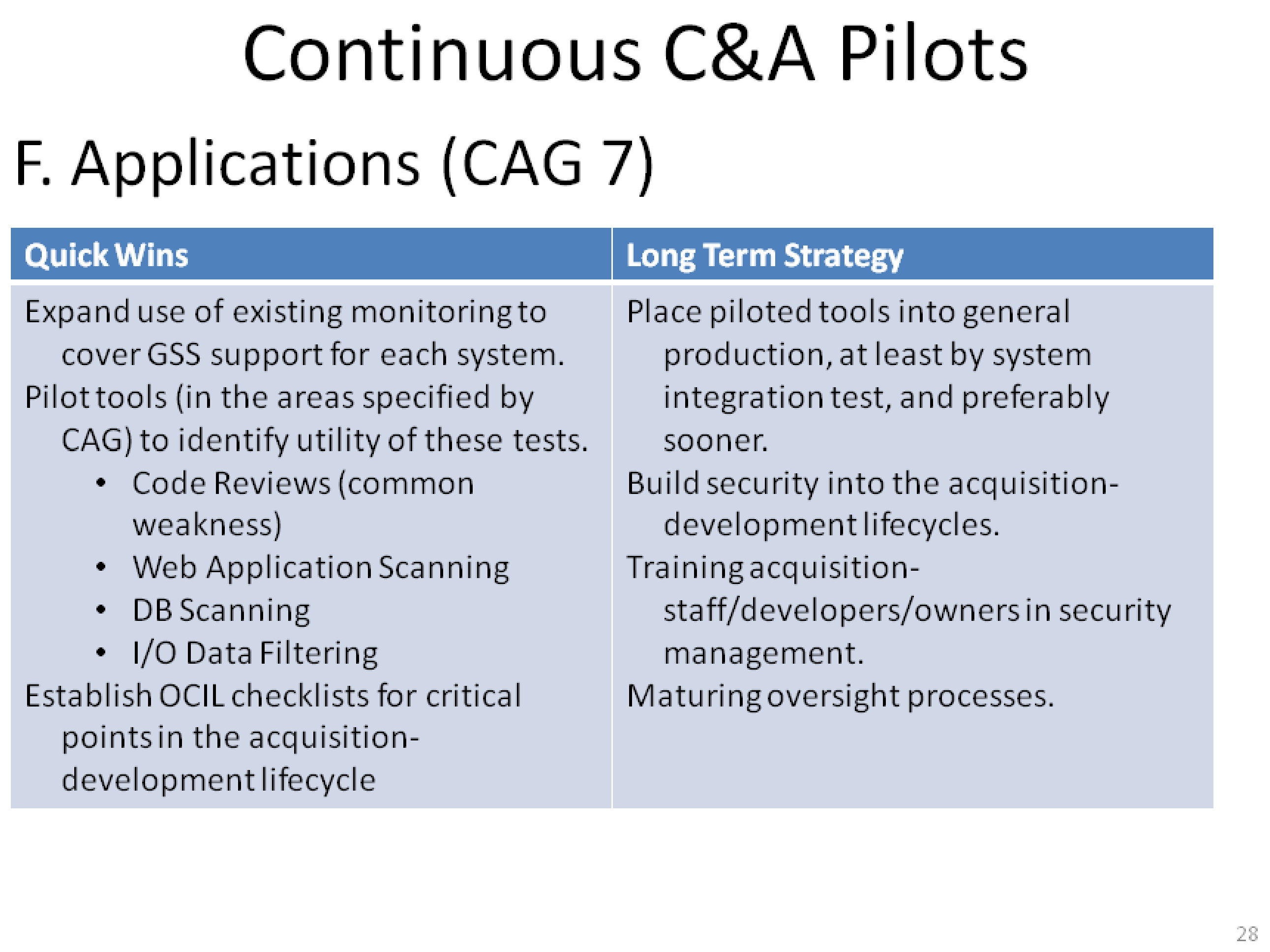


Continuous C&A Pilots

E. Situational Awareness and Threat Analysis

Quick Wins	Long Term Strategy
Situational Awareness: Conduct pilots to identify attack paths using GOTS tools and find ways to block attacks on parts of the network.	Using lessons learned from quick wins, expand to the full network, using a COTS tool, if appropriate. Use capability to refine risk scoring and inform the DAA decision process. Maturing oversight processes.
Threat Analysis: • Continue current practices. • Use Existing Threat Analysis capability to refine risk scoring. • Use DHS penetration team on any system late for C&A.	Find ways to refine these practices. Use to inform the DAA decision process. Maturing oversight processes.

F. Applications (CAG 7)

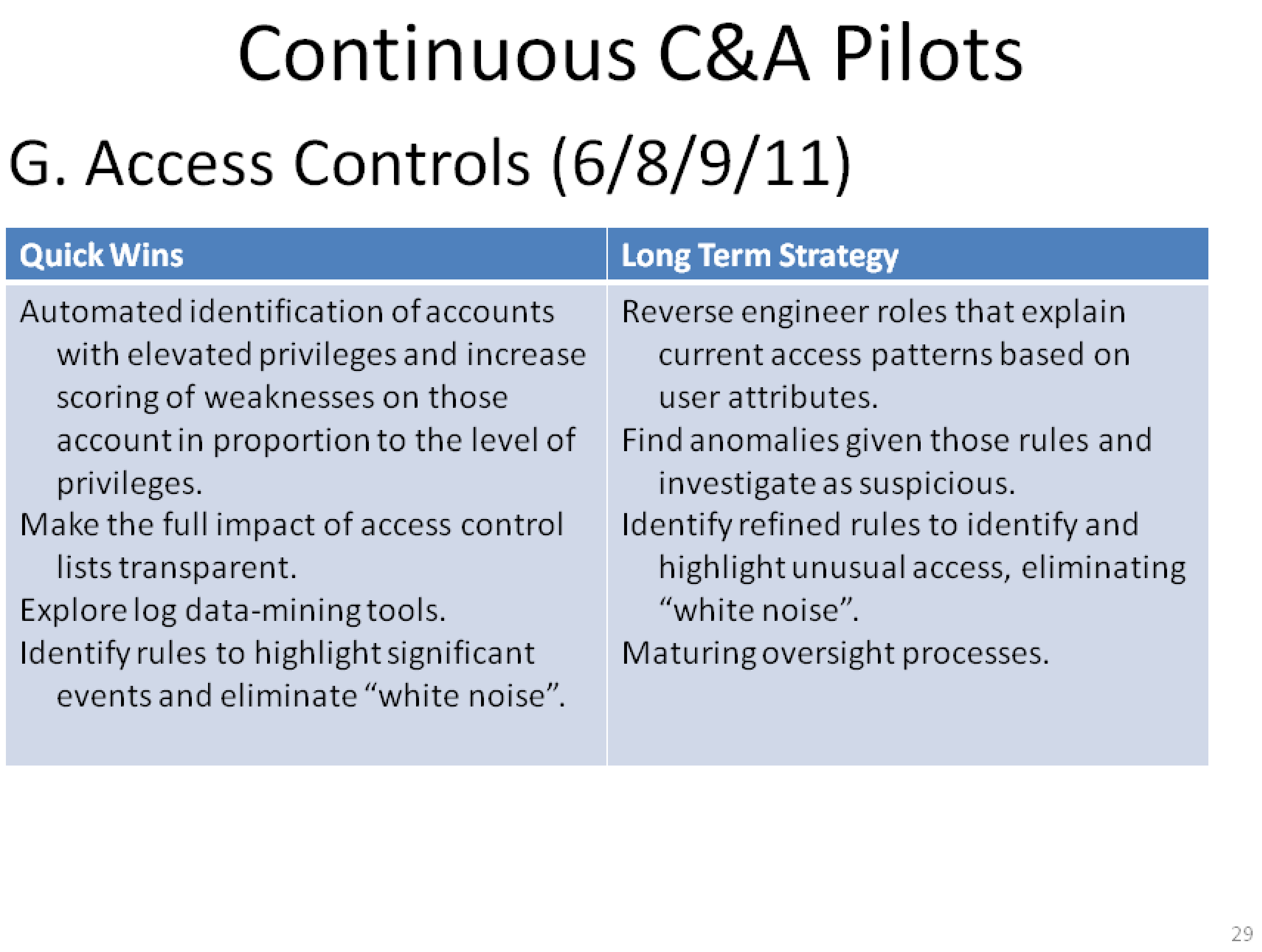


Continuous C&A Pilots

F. Applications (CAG 7)

Quick Wins	Long Term Strategy
Expand use of existing monitoring to cover GSS support for each system. Pilot tools (in the areas specified by CAG) to identify utility of these tests. • Code Reviews (common weakness) • Web Application Scanning • DB Scanning • I/O Data Filtering Establish OCIL checklists for critical points in the acquisition-development lifecycle	Place piloted tools into general production, at least by system integration test, and preferably sooner. Build security into the acquisition-development lifecycles. Training acquisition-staff/developers/owners in security management. Maturing oversight processes.

G. Access Controls (6/8/9/11)



Continuous C&A Pilots

G. Access Controls (6/8/9/11)

Quick Wins	Long Term Strategy
Automated identification of accounts with elevated privileges and increase scoring of weaknesses on those account in proportion to the level of privileges. Make the full impact of access control lists transparent. Explore log data-mining tools. Identify rules to highlight significant events and eliminate "white noise".	Reverse engineer roles that explain current access patterns based on user attributes. Find anomalies given those rules and investigate as suspicious. Identify refined rules to identify and highlight unusual access, eliminating "white noise". Maturing oversight processes.